WE CLAIM

1. A load balancing device for balancing the load across a plurality of proxy devices arranged to perform malware scanning of files stored within a file storage device of a computer network, the computer network having a plurality of client devices arranged to issue access requests using a dedicated file access protocol to the file storage device in order to access files stored on the file storage device, the load balancing device being arranged so as to intercept access requests issued to the file storage device, and comprising:

a client interface for receiving an access request issued to the file storage device using the dedicated file access protocol;

load balancing logic for applying a predetermined load balancing routine to determine to which proxy device to direct that access request; and

a proxy device interface for sending the access request to the proxy device determined by the load balancing logic, each proxy device being coupled to the file storage device.

2. A load balancing device as claimed in Claim 1, wherein the dedicated file access protocol is the Server Message Block (SMB) protocol, and the access requests are SMB calls issued to the file storage device.

3. A load balancing device as claimed in Claim 1, wherein the dedicated file access protocol is the Network File System (NFS) protocol, and the access requests are NFS calls issued to the file storage device.

4. A load balancing device as claimed in Claim 1, wherein said load balancing routine is arranged, upon receipt of an access request, to poll each of the plurality of proxy devices, and to cause the access request to be sent to the first proxy device in said plurality that replies with an indication that it is available to handle the access request.

5. A load balancing device as claimed in Claim 1, wherein said load balancing routine is arranged to apply a "round robin" system of allocation of access requests to proxy devices in said plurality so as to evenly distribute the access requests amongst the plurality of proxy devices.

6. A load balancing device as claimed in Claim 1, wherein the proxy device interface is arranged to receive a ready signal from each proxy device in said plurality indicating whether that proxy device is ready to receive an access request, the load balancing routine being arranged to refer to said ready signals when determining to which proxy device to direct a particular access request.

7. A load balancing device as claimed in Claim 1, wherein each device in the computer network is assigned an identifier, and the load balancing device is assigned the same identifier as is assigned to the file storage device, the client interface being connectable to a communication infrastructure of the computer network to enable communication between the load balancing device and said client devices, whilst the plurality of proxy devices are connectable to the proxy device interface and the file storage device is connectable to each proxy device, such that the file storage device is only accessible by said client devices via said load balancing device and one of said proxy devices.

8. A load balancing device as claimed in Claim 7, wherein a plurality of file storage devices may be connected to each of said proxy devices, each file storage device having a different identifier, and the load balancing device being assigned multiple identifiers corresponding to the identifiers of the file storage devices connected to the plurality of proxy devices, the client interface being configured to receive any access requests issued to one of said file storage devices connected to the plurality of proxy devices.

9. A load balancing device as claimed in Claim 1, wherein each device in the computer network is assigned an identifier, the load balancing device being assigned a unique identifier different to the identifier of the file storage device, the client devices,

the load balancing device and the file storage device being connectable to a communication infrastructure of the computer network, the client devices being configured such that access requests issued by the client devices are routed to the load balancing device, and the file storage device being configured to return each processed access request to the proxy device from which that access request was received.

10. A balanced proxy system for performing malware scanning of files stored within a file storage device of a computer network, the computer network having a plurality of client devices arranged to issue access requests using a dedicated file access protocol to the file storage device in order to access files stored on the file storage device, the balanced proxy system being arranged so as to intercept access requests issued to the file storage device, and comprising:

a plurality of proxy devices arranged to perform said malware scanning of files stored within the file storage device; and

a load balancing device as claimed in Claim 1 for determining to which of said plurality of proxy devices to direct any particular access request;

each proxy device comprising:

(a) a first interface for receiving from the load balancing device an access request issued by one of said client devices to said file storage device using the dedicated file access protocol;

(b) a second interface for communicating with the file storage device to cause the file storage device to process the access request;

(c) processing logic for causing selected malware scanning algorithms to be executed to determine whether the file identified by the access request is to be considered as malware.

11. A balanced proxy system as claimed in Claim 10, wherein the processing logic is responsive to configuration data to determine which malware scanning algorithms should be selected for a particular file, each proxy device further comprising a scanning engine to execute the malware scanning algorithms selected by the processing logic.

12. A balanced proxy system as claimed in Claim 10, wherein each proxy device further comprises a file cache for storing files previously accessed by the client devices, upon receipt of an access request identifying a file to be read from the file storage device, the processing logic being arranged to determine whether the file identified by the access request is stored in the file cache and if so to return the file to the client device via the load balancing device without communicating with the file storage device via the second interface.

13. A balanced proxy system as claimed in Claim 12, wherein the file cache is arranged only to store files which have been determined not to be considered as malware.

14. A balanced proxy system as claimed in Claim 10, wherein, upon receipt of an access request, the processing logic is arranged to determine from the access request predetermined attributes, and to send those predetermined attributes to the file storage device to enable the file storage device to perform a validation check, the processing logic only allowing the access request to proceed if the file storage device confirms that the client device is allowed to access the file identified by the file access request.

15. A balanced proxy system as claimed in Claim 14, further comprising a user cache for storing the predetermined attributes.

16. A method of operating a load balancing device to balance the load across a plurality of proxy devices arranged to perform malware scanning of files stored within a file storage device of a computer network, the computer network having a plurality of client devices arranged to issue access requests using a dedicated file access protocol to the file storage device in order to access files stored on the file storage device, the load balancing device being arranged so as to intercept access requests issued to the file storage device, and the method comprising the steps of:

(a) receiving an access request issued to the file storage device using the dedicated file access protocol;

(b) applying a predetermined load balancing routine to determine to which proxy device to direct that access request; and

(c) sending the access request to the proxy device determined at said step (b), each proxy device being coupled to the file storage device.

17. A method as claimed in Claim 16, wherein the dedicated file access protocol is the Server Message Block (SMB) protocol, and the access requests are SMB calls issued to the file storage device.

18. A method as claimed in Claim 16, wherein the dedicated file access protocol is the Network File System (NFS) protocol, and the access requests are NFS calls issued to the file storage device.

19. A method as claimed in Claim 16, wherein said load balancing routine is arranged, upon receipt of an access request, to poll each of the plurality of proxy devices, and to cause the access request to be sent to the first proxy device in said plurality that replies with an indication that it is available to handle the access request.

20. A method as claimed in Claim 16, wherein said load balancing routine is arranged to apply a "round robin" system of allocation of access requests to proxy devices in said plurality so as to evenly distribute the access requests amongst the plurality of proxy devices.

21. A method as claimed in Claim 16, wherein the load balancing device is arranged to receive a ready signal from each proxy device in said plurality indicating whether that proxy device is ready to receive an access request, the load balancing routine being arranged to refer to said ready signals when determining to which proxy device to direct a particular access request.

22. A method as claimed in Claim 16, wherein each device in the computer network is assigned an identifier, and the load balancing device is assigned the same identifier as is assigned to the file storage device, the method comprising the steps of:

connecting a client interface of the load balancing device to a communication infrastructure of the computer network to enable communication between the load balancing device and said client devices;

connecting the plurality of proxy devices to a proxy device interface of the load balancing device; and

connecting the file storage device to each proxy device, such that the file storage device is only accessible by said client devices via said load balancing device and one of said proxy devices.

23. A method as claimed in Claim 22, wherein a plurality of file storage devices may be connected to each of said proxy devices, each file storage device having a different identifier, and the load balancing device being assigned multiple identifiers corresponding to the identifiers of the file storage devices connected to the plurality of proxy devices, the client interface being configured to receive any access requests issued to one of said file storage devices connected to the plurality of proxy devices.

24. A method as claimed in Claim 16, wherein each device in the computer network is assigned an identifier, the load balancing device being assigned a unique identifier different to the identifier of the file storage device, the method comprising the steps of:

connecting the client devices, the load balancing device and the file storage device to a communication infrastructure of the computer network;

configuring the client devices such that access requests issued by the client devices are routed to the load balancing device; and

configuring the file storage device to return each processed access request to the proxy device from which that access request was received.

25. A method as claimed in Claim 16, wherein each proxy device is arranged to perform the steps of:

(i) receiving from the load balancing device an access request issued by one of said client devices to said file storage device using the dedicated file access protocol;

(ii) communicating with the file storage device to cause the file storage device to process the access request; and

(iii) causing selected malware scanning algorithms to be executed to determine whether the file identified by the access request is to be considered as malware.

26. A method as claimed in Claim 25, wherein said step (iii) comprises the steps of:

responsive to configuration data, determining which malware scanning algorithms should be selected for a particular file; and

employing a scanning engine to execute the malware scanning algorithms selected by said determining step.

27. A method as claimed in Claim 25, wherein each proxy device is arranged to perform the further steps of:

storing within a file cache files previously accessed by the client devices;

upon receipt of an access request identifying a file to be read from the file storage device, determining whether the file identified by the access request is stored in the file cache and if so to return the file to the client device via the load balancing device without communicating with the file storage device.

28. A method as claimed in Claim 27, wherein the file cache is arranged only to store files which have been determined not to be considered as malware.

29. A method as claimed in Claim 25, wherein each proxy device is arranged to perform the further steps of:

upon receipt of an access request, determining from the access request predetermined attributes;

sending those predetermined attributes to the file storage device to enable the file storage device to perform a validation check; and

only allowing the access request to proceed if the file storage device confirms that the client device is allowed to access the file identified by the file access request.

30. A method as claimed in Claim 29, further comprising the step of storing within a user cache the predetermined attributes.

31. A computer program product operable to configure a load balancing device to perform a method of balancing the load across a plurality of proxy devices arranged to perform malware scanning of files stored within a file storage device of a computer network, the computer network having a plurality of client devices arranged to issue access requests using a dedicated file access protocol to the file storage device in order to access files stored on the file storage device, the load balancing device being arranged so as to intercept access requests issued to the file storage device, and the computer program product comprising:

(a) client interface code operable to receive an access request issued to the file storage device using the dedicated file access protocol;

(b) load balancing code operable to apply a predetermined load balancing routine to determine to which proxy device to direct that access request; and

(c) proxy device interface code operable to send the access request to the proxy device determined by the load balancing logic, each proxy device being coupled to the file storage device.

32. A computer program product as claimed in Claim 31, wherein the dedicated file access protocol is the Server Message Block (SMB) protocol, and the access requests are SMB calls issued to the file storage device.

33. A computer program product as claimed in Claim 31, wherein the dedicated file access protocol is the Network File System (NFS) protocol, and the access requests are NFS calls issued to the file storage device.

34. A computer program product as claimed in Claim 31, wherein said load balancing routine is arranged, upon receipt of an access request, to poll each of the plurality of proxy devices, and to cause the access request to be sent to the first proxy device in said plurality that replies with an indication that it is available to handle the access request.

35. A computer program product as claimed in Claim 31, wherein said load balancing routine is arranged to apply a "round robin" system of allocation of access requests to proxy devices in said plurality so as to evenly distribute the access requests amongst the plurality of proxy devices.

36. A computer program product as claimed in Claim 31, wherein the load balancing device is arranged to receive a ready signal from each proxy device in said plurality indicating whether that proxy device is ready to receive an access request, the load balancing routine being arranged to refer to said ready signals when determining to which proxy device to direct a particular access request.

37. A computer program product as claimed in Claim 31, wherein each device in the computer network is assigned an identifier, and the load balancing device is assigned the same identifier as is assigned to the file storage device, a client interface of the load balancing device being connectable to a communication infrastructure of the computer network to enable communication between the load balancing device and said client devices, whilst the plurality of proxy devices are connectable to a proxy device interface of the load balancing device and the file storage device is connectable to each proxy device, such that the file storage device is only accessible by said client devices via said load balancing device and one of said proxy devices.

38. A computer program product as claimed in Claim 37, wherein a plurality of file storage devices may be connected to each of said proxy devices, each file storage device having a different identifier, and the load balancing device being assigned multiple identifiers corresponding to the identifiers of the file storage devices connected to the

plurality of proxy devices, the client interface code being operable to receive any access requests issued to one of said file storage devices connected to the plurality of proxy devices.

39. A computer program product as claimed in Claim 31, wherein each device in the computer network is assigned an identifier, the load balancing device being assigned a unique identifier different to the identifier of the file storage device, the client devices, the load balancing device and the file storage device being connectable to a communication infrastructure of the computer network, the client devices being configured such that access requests issued by the client devices are routed to the load balancing device, and the file storage device being configured to return each processed access request to the proxy device from which that access request was received.

40. A computer program product operable to configure a balanced proxy system to perform a method of malware scanning of files stored within a file storage device of a computer network, the computer network having a plurality of client devices arranged to issue access requests using a dedicated file access protocol to the file storage device in order to access files stored on the file storage device, the balanced proxy system being arranged so as to intercept access requests issued to the file storage device, the balanced proxy system comprising a plurality of proxy devices arranged to perform said malware scanning of files stored within the file storage device, and a load balancing device for determining to which of said plurality of proxy devices to direct any particular access request, the computer program product comprising:

a first computer program product as claimed in Claim 31 operable to configure the load balancing device to perform a method of balancing the load across the plurality of proxy devices; and

a second computer program product operable to configure each proxy device to perform said malware scanning, comprising:

reception code operable to receive from the load balancing device an access request issued by one of said client devices to said file storage device using the dedicated file access protocol;

communication code operable to communicate with the file storage device to cause the file storage device to process the access request; and

algorithm invoking code operable to cause selected malware scanning algorithms to be executed to determine whether the file identified by the access request is to be considered as malware.

41. A computer program product as claimed in Claim 40, wherein said algorithm invoking code is operable to determine, responsive to configuration data, which malware scanning algorithms should be selected for a particular file, and the second computer program product further comprises scanning engine code responsive to said algorithm invoking code and operable to execute the malware scanning algorithms selected by said algorithm invoking code.

42. A computer program product as claimed in Claim 40, wherein said second computer program product further comprises:

caching code operable to store within a file cache files previously accessed by the client devices;

the reception code being operable, upon receipt of an access request identifying a file to be read from the file storage device, to determine whether the file identified by the access request is stored in the file cache and if so to return the file to the client device via the load balancing device without communicating with the file storage device.

43. A computer program product as claimed in Claim 42, wherein the file cache is arranged only to store files which have been determined not to be considered as malware.

44. A computer program product as claimed in Claim 40, wherein said reception code is operable, upon receipt of an access request, to determine from the access request predetermined attributes, the communication code being operable to send those predetermined attributes to the file storage device to enable the file storage device to perform a validation check, the access request only being allowed to proceed if the file

storage device confirms that the client device is allowed to access the file identified by the file access request.

45. A computer program product as claimed in Claim 44, further comprising a user cache for storing the predetermined attributes.